CLAIMS

1. A communication apparatus for verifying validity of a server that is connected to said communication apparatus via a communication network, comprising:

a first storage unit operable to hold first CA information that includes a first CA certificate and a next address for update, the first CA certificate indicating that a server certificate that indicates the validity of the server is valid, and the next address for update indicating a location, on the communication network, of a download server on which second CA information is placed, said second CA information including a second CA certificate to be a next valid CA certificate in a case where said first CA certificate becomes revoked;

an authentication unit operable to authenticate the server by verifying the server certificate using the first CA certificate; and

a CA information update unit operable to obtain the second CA information from the download server indicated by the next address for update,

wherein when the first CA certificate becomes revoked, the authentication unit thereafter authenticates the server using the second CA certificate included in the second CA information obtained by the CA information update unit.

2. The communication apparatus according to Claim 1,

wherein the CA information update unit tries to connect to the download server periodically, and obtains the second CA information from the download server when said connection succeeds.

3. The communication apparatus according to Claim 1,

wherein the CA information update unit tries to connect to the download server when the authentication unit has failed to authenticate the server using the first CA certificate, and obtains the second CA information from the download server when said

connection succeeds.

4. The communication apparatus according to Claim 1,

wherein the authentication unit tries to authenticate the server using the second CA certificate included in the second CA information obtained by the CA information update unit, and when said authentication succeeds, thereafter authenticates the server using the second CA certificate instead of the first CA certificate.

5. The communication apparatus according to Claim 1, further comprising a second storage unit operable to hold the second CA information,

wherein the CA information update unit stores, into the second storage unit, the second CA information obtained from the download server, and

when the first CA certificate becomes revoked, the authentication unit thereafter authenticates the server using the second CA certificate included in the second CA information stored in the second storage unit.

6. The communication apparatus according to Claim 1, further comprising a second storage unit operable to hold the second CA information,

wherein the CA information update unit stores, into the second storage unit, the second CA information obtained from the download server, and

when the first CA certificate becomes revoked, the authentication unit moves the second CA information stored in the second storage unit into the first storage unit, and thereafter authenticates the server using the second CA certificate included in the second CA information stored in the first storage unit.

7. The communication apparatus according to Claim 1,

wherein the CA information update unit obtains, from the download server, a download server certificate indicating validity of said download server, and obtains the second CA information after authenticating the validity of the download server based on said obtained download server certificate.

8. A validity verification method for verifying validity of a server via a communication network, comprising:

a storage step of storing, into a recording unit, first CA information that includes a first CA certificate and a next address for update, the first CA certificate indicating that a server certificate that indicates the validity of the server is valid, and the next address for update indicating a location, on the communication network, of a download server on which second CA information is placed, said second CA information including a second CA certificate to be a next valid CA certificate in a case where said first CA certificate becomes revoked;

an authentication step of authenticating the server by verifying the server certificate using the first CA certificate; and

a CA information update step of obtaining the second CA information from the download server indicated by the next address for update,

wherein in the authentication step, when the first CA certificate becomes revoked, the server is thereafter authenticated using the second CA certificate included in the second CA information obtained in the CA information update step.

9. A program for a communication apparatus that verifies validity of a server connected to said communication apparatus via a communication network, the program causing a computer to execute the steps included in the validity verification method

according to Claim 8.

10. An authentication apparatus for ensuring validity of a server that is connected to said authentication apparatus via a communication network, comprising:

a server certificate issue unit operable to issue a server certificate that ensures the validity of the server; and

a CA information issue unit operable to issue first CA information that includes a first CA certificate and a next address for update, the first CA certificate indicating that said server certificate is valid, and the next address for update indicating a location, on the communication network, of a download server on which second CA information is placed, said second CA information including a second CA certificate to be a next valid CA certificate in a case where said first CA certificate becomes revoked.

11. An authentication method for ensuring validity of a server via a communication network, comprising:

a server certificate issue step of issuing a server certificate that ensures the validity of the server; and

a CA information issue step of issuing first CA information that includes a first CA certificate and a next address for update, the first CA certificate indicating that said server certificate is valid, and the next address for update indicating a location, on the communication network, of a download server on which second CA information is placed, said second CA information including a second CA certificate to be a next valid CA certificate in a case where said first CA certificate becomes revoked

12. A program for an authentication apparatus that ensures validity of a server connected to said authentication apparatus via a communication network, the program causing a computer to

execute the steps included in the authentication method according to Claim 11.

13. An operation method for operating a communication system comprising an Nth authentication apparatus, an (N+1)th authentication apparatus, and an (N+1)th download server which are connected over a communication network,

wherein the Nth authentication apparatus includes:

an Nth server certificate issue unit operable to issue an Nth server certificate that ensures validity of an application server; and

an Nth CA information issue unit operable to issue Nth CA information that includes an Nth CA certificate and an (N+1)th address for update, the Nth CA certificate indicating that the Nth server certificate is valid, and the (N+1)th address for update indicating a location of the (N+1)th download server on the communication network,

the (N+1)th authentication apparatus includes:

an (N+1)th server certificate issue unit operable to issue an (N+1)th server certificate that ensures the validity of the application server; and

an (N+1)th CA information issue unit operable to issue (N+1)th CA information that includes an (N+1)th CA certificate and an (N+2)th address for update, the (N+1)th CA certificate indicating that the (N+1)th server certificate is valid, and the (N+2)th address for update indicating a location, on the communication network, of an (N+2)th download server on which (N+2)th CA information is placed, said (N+2)th CA information including an (N+2)th CA certificate to be a next valid CA certificate in a case where said (N+1)th CA certificate becomes revoked,

the (N+1)th download server includes:

a CA information storage unit operable to hold the (N+1)th CA information that includes the (N+1)th CA certificate to be a next

valid CA certificate in a case where said Nth CA certificate becomes revoked; and

an output unit operable to output, to a communication apparatus, the (N+1)th CA information stored in the CA information storage unit, the communication apparatus being connected to said (N+1)th download server via the communication network, and

in the operation method, the following steps are repeated for N number of times, where N is 1 or a larger integer:

an Nth operation step of operating the Nth authentication apparatus; and

an (N+1)th operation step of operating the (N+1)th authentication apparatus and the (N+1)th download server before a validity period of the Nth CA certificate expires.

14. The operation method according to Claim 13,

wherein in the (N+1)th operation step, the (N+1)th authentication apparatus and the (N+1)th download server are operated, in a case where the Nth CA certificate becomes revoked.

15. The operation method according to Claim 13, further comprising a termination step of terminating the operation of the Nth authentication apparatus and the operation of the (N+1)th download server, when a validity period of the Nth CA certificate expires.